ENHANCED SECURITY ASSESSMENT IN CYBER PHYSICAL SYSTEMS USING MACHINE LEARNING TECHNIQUES

A SYNOPSIS

Submitted by

S.KRISHNANARAYANAN
(Reg. No. 201907173)

in partial fulfillment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

SCHOOL OF COMPUTING

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMIL NADU, INDIA

FEBRUARY 2024

Introduction

Bringing together computing and physical capacity, cyber physical systems (CPS) interact with humans in novel ways. It is not intended to function independently, but rather as a network of several variables with both physical input and output. Concepts like this have direct ties to computational intelligence-based sensor networks, which are increasingly used in fields like robotics. Embedded systems, which incorporate transdisciplinary strategies, mechatronics, and design, are essential to the functioning of any cyber physical system. As a result, Cyber Physical Systems are ubiquitous in fields as diverse as manufacturing, aerospace, automotive, transportation, etc., each representing a unique blend of physical and computational aspects. The term "Cyber-Physical System" (CPS) refers to any computer system in which algorithms are used to control or monitor a physical mechanism. Physical and software parts of cyber-physical systems are intricately interwoven; they can function on different geographical and temporal dimensions, display diverse and unique behavioural modalities, and interact in context-specific ways. The term "cyber-physical system" (CPS) refers to any system that combines hardware, software, and maybe even more types of systems (e.g., human systems). All these are interconnected and work together to produce a global pattern of behaviour. As a result, CPS will typically consist of both complicated software components and hardware components like sensors, actuators, and similar embedded systems that interact with the physical environment. Transdisciplinary methods are utilised in CPS, which integrates the fields of cybernetics, mechatronics, design, and process science. Embedded systems are commonly used in process control.

2.Literature Review

For "the next model of approach which requires sparse integration of control technologies, communication, and computing to get equilibrium, robustness, reliability, performance, and then productivity inside battling genuine physical devices of numerous programme domains," CPS is the way to go. Because of their widespread application, CPSs have been the focus of several committee meetings and reports aimed at identifying and addressing potential future challenges and opportunities Dai, et al.**[1]**. Devices for the general public are everywhere; cell phones, video players, and gaming systems all respond to voice commands, and there are even wearable gadgets. Intelligent buildings feature high-tech sensors, ubiquitous media, and efficient energy management. New medical technologies have the potential to improve treatment adherence while decreasing overall healthcare costs. A brand new power programme process dubbed the "smart grid" offers to use CPS solutions to improve configurability, adaptability, self-management, and responsiveness, but will simultaneously need CPS breakthroughs in security to computer monitor, control, and also circumvent risks all on its own.

Scheduling and balancing challenges inside highly diverse CPS may be considered as members of the same family of NP-complete problems that arise in both general and restricted settings Qiao,et al.**[2]**. The field of computer science known as distributed computing involves studying remote approaches. Networked computers host the procedures of a distributed technique, coordinating and communicating their operations via the use of exchanging communications to achieve a common goal Yang, Huang Pen & Zhang**[3].** Cloud and internet knowledge have allowed for the development of the procedures to reach full maturity Fei,et al.**[4]**

The actual physical properties of the technique dictate the amount of threads that mayrun within the devices. In addition, there are already customary restrictions mandated by software requirements, such as QoS, latency, or power consumption Qi, et al**[5]**.The field of computer science known as distributed computing involves studying remote approaches. The concept of a pervasive network, pervasive computing, advantage computing, and communal computing, among others**.** Khosravi, & Menon **[6].** In the field of machine learning, and more especially using Neural Networks, several different types of detectors have been created (NN). An unsupervised method for CPS anomaly detection using RNNs and a cumulative sum model Goh,et al.**[7].**

To address this issue, Kosek **[8]** suggested a NN-based contextual AD strategy for smart grids. Secondarily, Krishnamurthy et al Krishnamurthy, et a**l.[9].**used Bayesian networks. In the context of Bayesian networks, this is a model for discovering unlabeled relationships between cyber and physical variables across time. The goal of this work is to offer a novel perspective on dependability evaluation in the context of CPS and to explore the potential impact of emerging data infrastructures and data sources. We go into the three major components of CPS dependability—hardware dependability, software dependability, and the impact of human interaction on dependability—and discuss the prospect of information Zhou,,et al.**[10].** Using examples from two widely used CPS, smart factories and smart buildings, we further explain our main principles. Initially, we provide some context on CPS and trustworthiness assessment.

2.1.Challenges of deployment of CPS

Maintainability is a system's resilience, or its capacity to recover from failure. High maintainability of a system means that it can be fixed easily and quickly with little waste of supporting resources and no new issues arising as a result of the maintenance. We can suggest autonomous predictive/corrective diagnostic procedures if there is tight contact between the system components

Availability means that a system can still be accessed by users despite malfunctions. In order to be considered highly available, a system needs to be able to separate a failing component from the rest of the system and continue working without it. The availability of system services is seriously called into doubt by malicious cyberattacks.

Safety is the capacity of a system to function without endangering others in its vicinity. A highly secure system will comply with all relevant safety rules to the fullest degree possible and will have fail safes in place to prevent catastrophic failures.

Resilience is the ability of a system to continue functioning and providing services at a satisfactory level despite being subjected to faults of varying types. Resilient systems can identify faults quickly, repair themselves, and recover quickly so they can keep up with service demands. The need for strong resilience becomes more pressing if the application in question is mission-critical (e.g., automated brake control in vehicular Cyber-physical systems).

2.2.EXISTING SOLUTIONS OF SECURITY CHALLENGES IN CPS

There are a number of obstacles that must be overcome before any CPS application can be deployed. This may be accomplished by using a methodical approach at each stage of application development, from conceptualization to rollout. Multiple techniques and technologies have been presented to address the problems that arise at each step.

Security issues can be avoided in a number of ways, including the implementation of a context-aware security framework for CPS that employs dynamic adaptability to the physical environment with the aid of context coupling; the use of distributed real-time software; the use of competitive and cooperative resource management; the use of virtual test beds; the use of highly confidential software; the use of simulation and emulation platforms; and the conduct of experiments

3.Research Problem

Challenges encountered in CPS

The capacity of a system to reliably carry out its intended functions without observable decline in result or performance during operation is known as dependability. The degree to which individuals may have faith in the overall system is shown by its **dependability**. High reliability in a system means that it functions as intended, has no disruptions, and doesn't crash while carrying out its work.

The term "**accuracy**" refers to how closely the observed values of a system correspond to the computed ones. A highly accurate system should provide results that are as near to reality as feasible.

To be **efficient**, a system must minimise the amount of time, money, and other inputs that it takes to carry out its intended tasks. Highly efficient systems function accurately and make the most of their available resources

The **capacity** to survive under a wide range of environments is known as robustness. The sensors must often be deployed in the real world, where they must contend with a wide range of situations.

Challenges with Communication Network:

For CPS applications to be deployed, a communication network must be set up to bridge the gap between the real world and the virtual one.

Wired network: It is challenging to construct CPS applications utilising wired network. The vast majority of these programmes rely on wireless connections. If wires are utilised, the expense of doing so has a significant impact on how quickly a programme can be rolled out.

Challenges with Computation and Control Operations:

Both precision and timeliness are crucial in CPS applications. The value of data for decision-making will be lowered if it is not accurate or timely, even if an application can swiftly locate and analyse the data and retain it in the appropriate context for the audience that will be consuming the information. This difficulty is present in all data analysis,

To visualise data, we need to grasp it in its raw form, and if the use of CPS necessitates data analysis, this demands a great deal of knowledge. We need to know who the person is in the broadest sense, like a customer utilising a certain set of products, and what you're hoping to visualise out of the data if, for instance, your application requires user identification based on data extracted from social network material. In the absence of background information, visualisation tools are less likely to be useful.

4.RESEARCH OBJECTIVES

- To define a computational model that is shareable in a CPS enabled environment.
- To analyze the performance of CPS through ML based dependability analysis algorithm
- To monitor the abnormality in CPS using intelligent ML.

5.PROPOSED METHODOLOGY

Contribution 1:

A SHARED COMPUTATIONAL MODEL USING DISTRIBUTED PROCESSING IN A CPS ENABLES ENVIRONMENT

Combining computers, interaction, and equilibrium solutions [shih], CPS is a networked real physical unit process. The task processing section of CPS makes use of transmitted technologies, and it places an emphasis on the interconnection between objects, machines, and people on the basis of environmentally friendly attention, which is secure, reliable, and cost-effective real-time detection or maybe command of an actual entity.

MODELING CHALLENGES

Problem 1: Models with Nondeterministic or Zeno Behavior that Require a Solver State machines, dataflow models, synchronous/reactive models, and/or dynamical systems (DE) may be used to explain the computational aspects of a CPS that combine physical processes represented by continuous-time models of dynamics. Numerical approximations of the solutions of differential equations are used by solvers in continuous-time models.

Second, maintaining uniformity across model parts: Last part, we built a basic tank model and ran it through its paces in a situation that has no bearing on the actual world but serves as a good regression test for the model. Sadly, in reality, test scenario models are often forgotten. As they develop into more sophisticated, lifelike models, the need for a nave regression analysis fades away.

MODELING AND SIMULATIONS

Use of models, simulations, and demos in the engineering and development of complex systems is not new. With this context in mind, a figure1 is shown with a model is a representation of a natural or artificial entity that is an abstraction of the original by the deliberate simplification and exclusion of details. This means that there isn't a single "model" form that must be used. They range from formal descriptions to real items to computer simulations. Models are used in simulations when they are meant to stand in for the actual thing being simulated. By simulating the original, one may learn important details about its nature, behaviour, coherence, etc. Furthermore, simulations are used to either ascertain or affect user conduct. The simulation, like the model, may be carried out in either the real world or on a computer. If the model and simulations run with express purpose of visualising functions and modes of operation, then the word demonstrator is usually employed. The demonstrator acts as a boundary object that serves as a point of reference for all interactions, not only those between users and the simulated system.

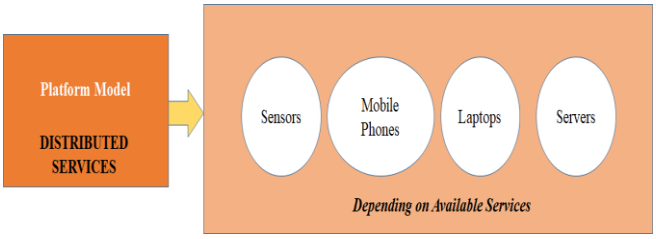

Figure 5.1: Platform Models

PROPOSED METHDOLOGY

This subfield of computing is defined by the way in which data is processed in real time by several components working in parallel with one another and with external input. This architecture is designed to manage the computer system in charge of dividing up the various application-related tasks. The module provides the appropriate approach to modelling CPS locations and enables one to ascertain the efficient distribution of tasks according to numerous objective characteristics. The introduced nomenclature is used to precisely identify the intended applications and the essential components upon which the proposed solution is predicated.

Figure 5.1 depicts a time series of a single instance of the general process to illustrate the core idea. This is an easy variant on the theme of an intelligent lighting scheme for smart cities. By using this software, urban streetlights may be activated or deactivated in response to the presence of moving cars or people. State-of-the-art form analysis functions on man identification in videos and photos make use of the software decomposition and the precise occupations mentioned by this example. An intelligent sensor, a mobile device, and a cluster of servers make up this instance software.

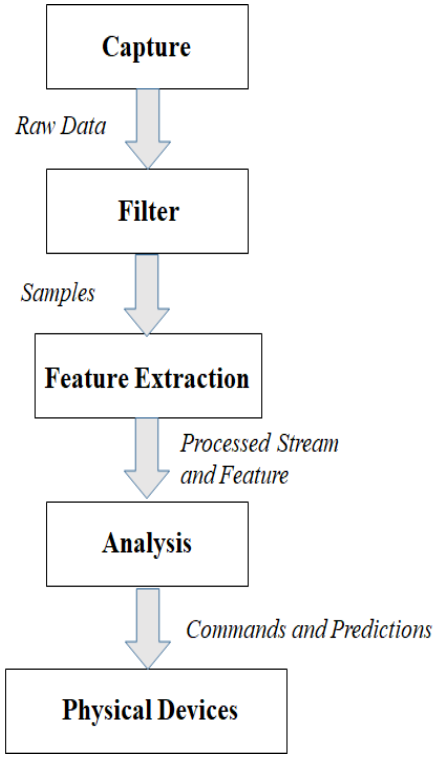

Figure 5.2: Data Flow Diagram

Targeted Applications

Figure 5.2 shows a data flow diagram of the previously sent programme that was modelled using this concept. Data from real-world receptors is analysed in accordance with a predetermined methodology, and examples of routine data processing tasks involving electronic signals are provided within the framework of a possible CPS

Application Specification Resources

Consistent with the specification of the domain, we establish C as a collection of computer hardware on which different examples of projects in T may run. The C set is developed by the CPS's computer operating systems and the readily available cloud computing assets. This is a sample of a functional environment where the product might be used. If the sort of potential products that may predominate at any point of the system is accounted for throughout the design phase, this architecture may be able to endure significant computational power. You may simulate different CPS node types by treating function as if it were a node type. Realizing nodes, systems, server clusters, PCs, Macs, Linux, smartphones, tablets, wearables, etc. Each and every C-unit may now be defined as a "kind of" in this manner. Figure 5.3 depicts an example of numerous nodes, starting from the installed infrastructure, the available equipment, and the used cloud online resources. A proper characterization of the source consumption of the os's is necessary for efficient material distribution.

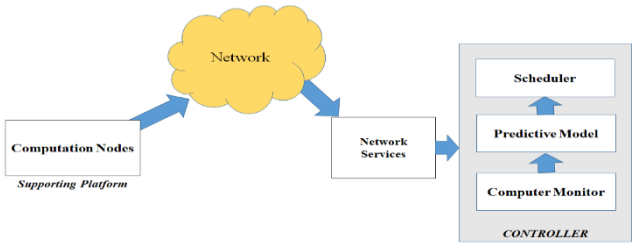

Figure 5.3: Numerous Nodes

PROPOSED SCHEME

Based on the available online resources, the processing needs, and the preferences of the end-user, a recommendation is provided on how to best operate the programme and its projects on the system's compute nodes. This management process is comprised of two main parts: (I) local proxy tasks running on each computation node in the system (which we refer to as "changes"), and (II) a process controller that monitors the entire telecommunications

network and provides various framework components such as discovering new nodes, testing existing ones, and setting up the source and the destination computer for each vital data flow. In order to cut down on the costs of handling communication and to conserve mentioned approaches, it is likely that they are offered in a centralised way. On a CPS with enough power and most of the nodes, the device controller might be hosted in the cloud or on another user's Pc. Figure 5.4 represents proposed schemes.

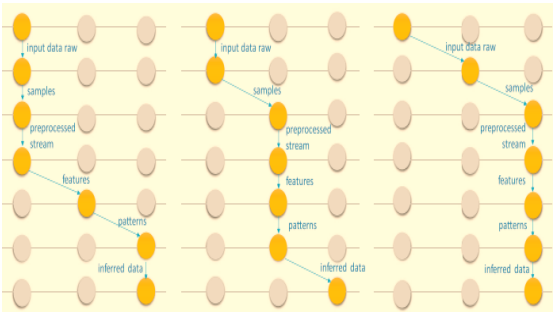

Figure 5.4: Proposed Schemes

Contribution 2

ANOMALY DETECTION IN CPS THROUGH EFFECTIVE PARAMETER TUNED DBN

Sensors used in CPS for the purpose of facility monitoring and management are especially vulnerable to anomalies such as scalability failures, cyber-attacks, and other incursions. In order to detect anomalies and stop harmful actions, a powerful model called ADS has been used. False Positives (FP) also known as false alarms and False Negatives (FN) also known as missed forecasts are both experienced by ADS despite its great efficiency. In CPS models, it often detracts from performance. In particular, recovery is performed when it is not necessary after using FP, but is skipped over by FN. Due to the inaccuracy of these forecasts, the managers receiving the numbers have less leeway to implement controls that maximise efficiency. In the end, it slows everything down. Figure 5.5 shows Intrusion Detection System of CPS

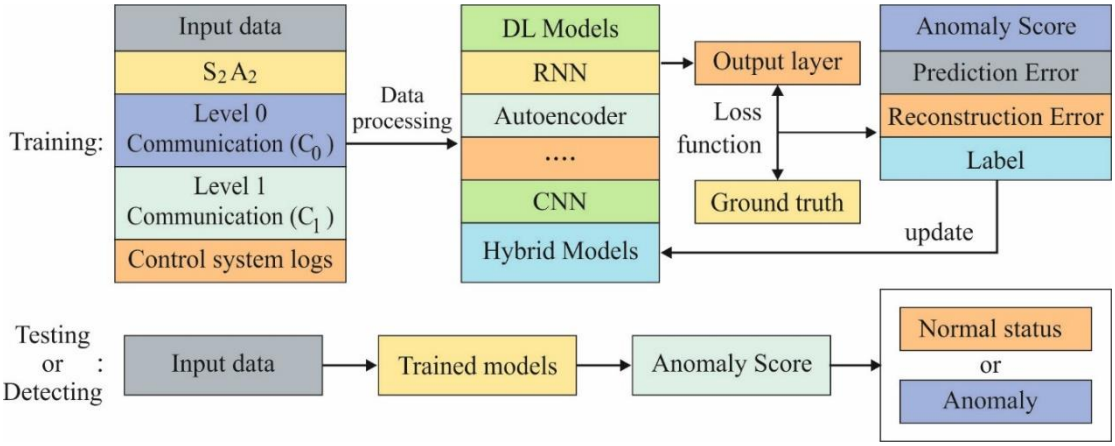

Figure 5.5: Intrusion Detection System of CPS

Models Of CPS

Systems that combine computing with physical processes are known as cyber-physical systems (CPSs). Control and monitoring of physical processes are handled by embedded computers and networks, which often employ feedback loops in which the physical processes influence the calculations and vice versa. That's why it's important to know how computers, programmes, networks, and physical processes all interact with one another when designing such systems. What distinguishes this field is the attention it pays to the dynamics of joints. Problems of central importance arise in the study of CPS that are uncommon in so-called general-purpose computing.

Models of Computation

The complexity and variability of CPS applications underlie some of the difficulties. The complexity of models can be reduced by employing models that are tailored to a particular domain and by employing modelling languages with well-defined semantics. The presence of heterogeneity calls for the integration of several different models. Models need to be constructed with well-defined MoCs [Edwards] to solve the first of these problems. By specifying whether model components run simultaneously, whether they share a common concept of time, and whether and how they share state, a MoC provides semantics to concurrency in the model

Abstract Semantics

Using a single, generic MoC for a complete design sometimes precludes the ability to verify properties in any way other than through prolonged simulation. MoCs with fewer features (less

expressiveness) are easier to analyse, leading to more thorough investigation of the design's attributes and, in many cases, formal verification. However, less evocative MoCs are unable to portray the complexity, nuance, and richness of modern design. The answer lies in a combination of several types of MoCs. In fact, due to the diverse nature of CPS applications, the use of various MoCs is often required. Moreover, the design process involves a wide range of abstraction, intricacy, and specificity in many design components. Engineers working on the project will bring a variety of expertise and perspectives to the table.

Auto-Oriented Models

An actor-oriented software component model [chicago], [E A Lee] is widely used in model-integrated development for embedded systems [Jan], [Karsai]. Actors are software components that run in parallel and exchange information via messages sent between ports in a distributed computing approach. The primary difficulty is delivering semantically rich actor-oriented MoCs. As a result, software's semantics are more often than not an afterthought, rather than an intentional design choice. Integrating actor-oriented models with realistic and useful concepts of time is a significant difficulty. Challenge 5 involves simulating dispersed behaviours, and to do this, it is necessary to give many temporal representations. Simulink and Modelica are two examples of modelling frameworks that incorporate a semantic notion of time, and both of these frameworks make the assumption that time moves in a consistent manner across the whole system.

Importance of Security in CPS

As the corporate sector has become increasingly reliant on digital transformation, the risk of cyberattacks against digital assets has grown. To strengthen their cyber security, organisations at high risk of data breaches should integrate cyber-physical systems into their overall strategy

Applications of CPS

Green Buildings: The greenhouse effect is a serious issue nowadays. 70% of all power generated is used by older structures, and these same buildings also emit the greenhouse gases that contribute to the greenhouse effect. We can reach our Zero Net Energy objective by utilising a coordinated network of wireless sensors, a central manager capable of cognitive processing, and a set of tightly regulated control systems.

Medical CPS: A crucial requirement for high-confidence medical cyber-physical systems is the integration of computation and control mechanisms to the essential medical information provided, which is gathered through wireless sensor networks.

Aeronautic applications: Aeronautic applications that make use of Cyber-Physical Systems include flight test instruments, pilot-crew communications, Structure Health Monitoring, In-Flight Tests, In-Flight Tests, In-Flight Entertainment Wireless Cabin, Flight Landing, etc.

1.1 Research challenges of CPS

A. General CPS security challenges

a) **Security by Design:** Given that most CPS are not linked to larger networks like the internet, they are not often built with security in mind. Because of this lack of interconnectivity, most CPS are built without any consideration for security. So, ensuring people's physical safety was nearly paramount.

b) **Cyber Physical Security:** So, ensuring people's physical safety was essentially paramount. In order to ensure the safety of CPSs, designers will need to adjust their perspective on security to include both cyber and physical threats. In the future, this might aid in the detection and prevention of cyberattacks with real-world effects. Both the cyber and physical components of the solution need to have previously neglected infrastructure built for them.

Requirements of open CPS

Specifically, the open CPS platform must meet the following requirements:

App Middleware: This will have methods for interacting with dynamically loaded applications. Its primary function is to allow apps to talk to each other, but it must also safeguard access to vital resources.

Reliability Regimes and Privacy Policies: To address threats to security and safety. For the secure and risk-free operation of safety-critical applications, the CPS platform should provide support for several reliability regimes. This category includes settings like fail-operational, fail-safe, and fail-secure.

Numerical type normalization

Normalization of numerical data is crucial in every dataset. Another possibility is that the value of characteristics varies among records in a dataset. When used to a classification problem, normalization improves performance by combining features from several dimensions and comparing them to a predetermined standard. After data normalization is performed, the previously irrelevant attribute values of the previously stored features become meaningful.

$$x_{scale} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

If x is a recently observed attribute value, x min represents the minimum value, x max represents the maximum value, and x scale determines the measure after attribute matching is complete.

DBN based Classification

To begin with, the limited Boltzmann machines were trained using a layer-wise greedy approach (RBM). Because DBN is a model for generating probabilities, it is often used in conjunction with other RBMs

It's a special example where the means of energy production may also serve as a learning model for data that's spatially dispersed in whatever way you choose..Figure 5.6 shows the structure of RBM.

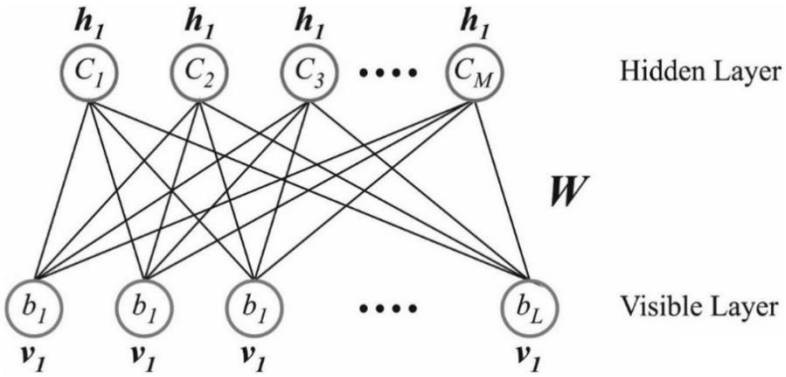

Figure 5.6 Structure of RBM

All RBMs feature what is called a "visible layer" and a "hidden layer," which consists of a bidirectional connection weight between the "visual" and "hidden" units. The combined energy function of each visual unit and hidden unit (v,h) is stated as where v is the visual unit, h is the hidden unit, w is the weight matrix, t is the visible unit threshold, and tb is the hidden unit threshold:

$$v = \{v_1, v_2, v_3, \dots, v_I\} \in \{0,1\} \quad (3)$$

$$h = \{h_1, h_2, h_3, \dots, h_I\} \in \{0,1\} \quad (4)$$

$$E(v,h) = -\sum_{i=1}^{I} a_i\, v_i - \sum_{j=1}^{J} b_i\, h_i - \sum_{j=1}^{J}\sum_{i=1}^{I} w_{ji}\, v_i h_j \quad (5)$$

as far as the quantity of receptive fields is concerned. I represents the ith digit of the image's numerical representation. The number of undetectable units is denoted by J. j represents the jth arbitrary pixel value. Consequently, the probabilities in both the hidden and the visible layers are distributed equally.

$$p(v,h) = \frac{e^{-E(v,h)}}{Z} \tag{6}$$

$$Z = \sum_{v}\sum_{h} e^{-E(v,h)} \tag{7}$$

where Z stands for the constant of the physical scheme that inspired the inspiration, and where the energy values between the visible and concealed layers may be used to get this constant. Similarly, if the hidden layer vector h is obtained as follows, then the input visual layer vector v may be constructed from the arbitrary hidden layer vector h.

$$p(h/v) = \prod_{j} p\,(h_j = 1/v) \tag{8}$$

$$p(v/h) = \prod_{j} p\,(v_i = 1/h) \tag{9}$$

$$sig(x) = 1/1 + e^{-x} \tag{10}$$

$$p\big(h_j = 1/v\big) = sig\left(b_i + \sum_{i}^{'} v_i\, w_{ji}\right) \tag{11}$$

$$p(v_i = 1/h) = sig\left(a_i + \sum_{j}^{J} h_j\, w_{ji}\right) \tag{12}$$

.

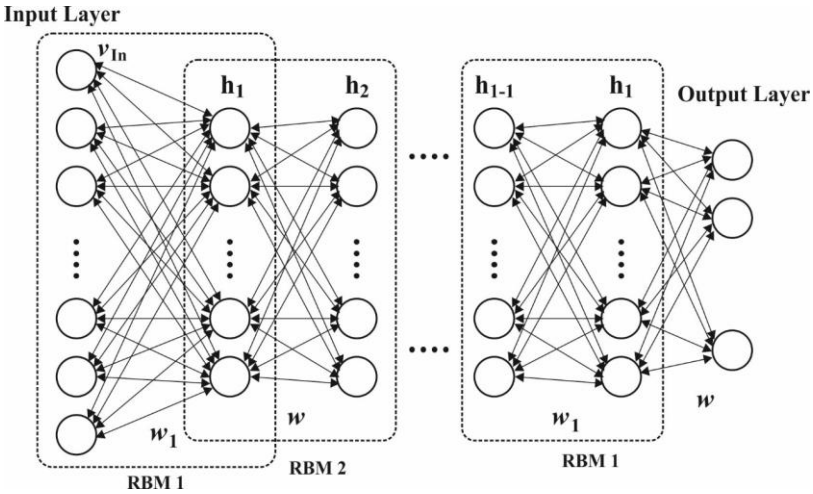

Figure 5.7. Architecture of DBN

In comparison to other models, the figure 5.7 shows the primary distinction in DBN training is the use of unsupervised layer-by-layer pre-training.

It may be trained to perform non-linear, complicated functions by directly mapping input to output. Next, a reliable feature extraction technique is of paramount importance. In the first phase, a vector was created in a higher-level RBM visible layer, and the RBM network's hidden layer was guaranteed to be valuable. After that, the visible layer is recreated using the concealed layer. The weights from the hidden layer and the visible layer have been extended till reaching the maximum iterations based on the difference between the rebuilt layer and the visual layer.

SSA based Parameter Tuning

Gliding is an effective technique used by microscopic animals for migration, and it mimics the dynamic foraging habit of southern flying squirrels [jain]. Squirrels adapt their habitat by gliding from tree to tree in the forest in search of food when temperatures are high. It has little trouble locating the vitamin-rich acorn nuts.

Initialize the Algorithm Parameters

Scaling factor, gliding constant, upper and lower constraints on decision variable FS U and FS L, and the probability of a predator's presence P dp are all crucial features of SSA. The figure 5.8 shows all the sequential steps In the first step of the SSA principle, all variables are held constant.

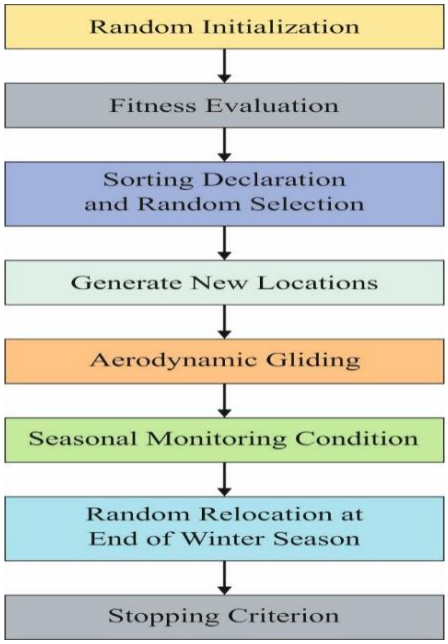

Figure 5.8:Flowchart of SSA

Contribution 3

DEPENDABILITY ANALYSIS ON CPS USING MACHINE LEARNING TECHNIQUES

The sensing level is made up of the sensory faculties of the physical world and the sensing faculties that are attractive to the end-user, while the collecting level is made up of various types of receptors, collectors, and terminals that have self-awareness and delivery skills. The cognitive layer performs a number of computations on the collected sensory data, and then uses more in-depth modelling, analysis, and reasoning to get a better understanding of the physical world, before relaying its findings to the management layer of the information network. Self-awareness, adaptability, controllability, intelligence, self-healing, integration, and safeguards [calva] are all features of CPS.

Within the service-oriented CPS structure created with a guidance on the architectural idea, the many CPS sources are divided into four distinct tiers. Starting at the bottom, these layers are the "service," "resource," "network," and "node" layers, respectively. The systematic community has recently been interested in the research hubs of academics both domestic and foreign. In a nutshell, complex physical systems (CPS) are multi-dimensional methods that mix physical, communication, and computational environments. The system type programme is an elaborate distributed software application procedure that makes cross-device and cross-platform component references. Reliability at an exceptionally high level is required to guarantee that the gadget can remain in a reliable programme propose at all times. Cyber physical systems, which are characterised by a close integration and coordination of computational and physical components, need a high level of system dependability.

METHDOLOGY

ML based Dependability both predicts the reliability of CPS and abstracts the application elements of the CPS process. Figure 9 shows the CPS infrastructure As a whole, the process consists of four phases: In the first level, which may be the CPS application phone's understanding stage, To better understand the attributes on the disappointment sequence of CPS software and to find accurate and appropriate prediction model, we must first have an understanding of how the CPS software is delivered to the device, in conjunction with the concept of CPS application structure. The fourth step is to evaluate and analyse the prediction model, which includes looking at the CPS program's results for predicting reliability over long time periods and comparing those results to the results from the manual model. While most

reliability-related operations have been well defined around hardware, they remain mostly undefined inside the programme, especially in terms of the language used to quantify them.

Dependability Analysis Algorithm:

For all CPS Components C

Calculate the number of Devices D

end **For**

Analyse the Dependability DA

DA = CPS (D) + ML

if DA = 0, Analysis Done and no issues

Continue the CPS Communication process

else

Not repeat the analysis till it gets no issue

end if

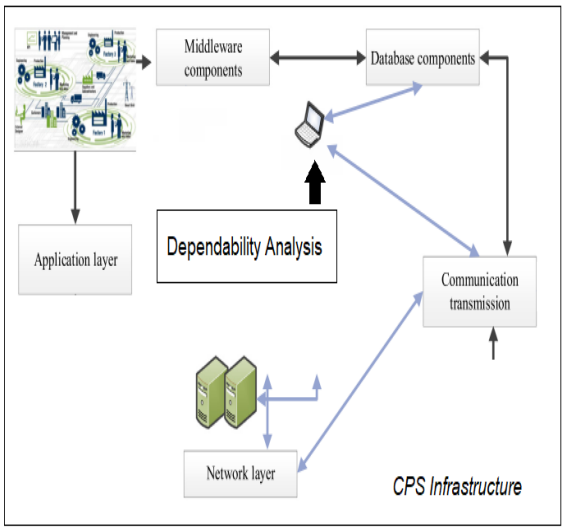

Figure 5.9:CPS Infrastructure

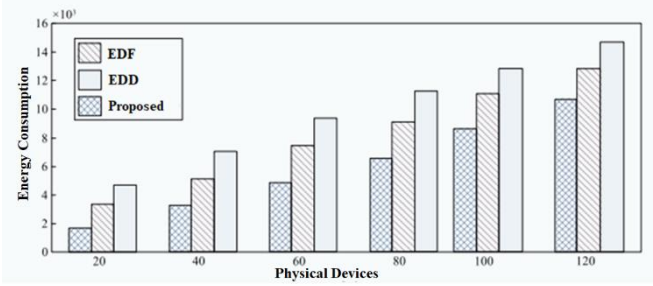

Figure 5.10: Energy Consumption

RESULT EVALUATION.

EVALUATION OF SHARED COMPUTATIONAL MODEL

This streaming section discusses the results of the experiments. This arrangement is well-grounded, as is the systematic discussion of the typical profile problem. Figure 5.10 shows the energy consumption. Each node uses the key between the sub and the absolute to play the matching ability of its, conserve components online resources, and conduct a few penalties and rewards on fiscal energy so that each state it creates on the intensity achieves well-balanced benefits. Specifics of the node's expression will be reflected in the feedback, both negative and positive. As a result, a heuristic algorithm was the only viable option for undertaking the task of work scheduling.

EVALUATION OF ANOMALY DETECTION IN EPTDBN BASED CPS.

Detection analysis of the proposed SSA-DBN model is explored in terms of several metrics, Fig. 5.12. With a maximum precision of 97.89%, recall of 98.91%, F-measure of 98.10%, and accuracy of 98.32%, the SSA-DBN model has successfully recognised DoS assaults. The SSA-DBN approach has also been shown to be superior at predicting R21 assaults, with a 98.93% accuracy, 99.15% recall, 99.04% F-measure, and 99.12% accuracy.

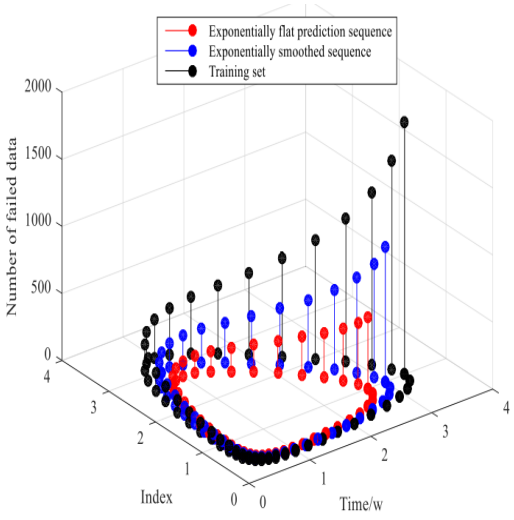

Figure 5.11:Result Analysis

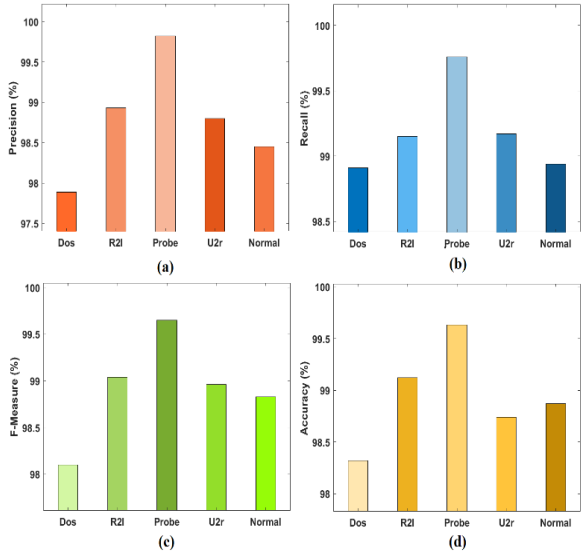

Figure 5.12:SSA-DBN Result Analysis

Figure 5.11 shows the Result Analysis. After that, Figure 5.12 shows the SSA-DBN method has recognised attacks with a maximum of 98.45% precision, recall of 98.94%, F-measure of 98.83%, and accuracy of 98.87% during an analysis of Normal attacks.

DEPENDABILITY ANALYSIS ON CPS PERFORMANCE EVALUATION

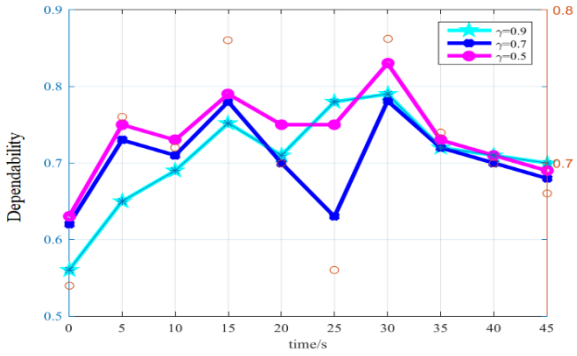

Figure 5.13: Dependability analysis on CPS

Figure 5.13 shows the dependability. The test kicks off a mobile device by using information classification, a redundancy check, and trend analysis, all of which are implemented using the SLM simulation wedge and the Mathlab ML software. Eighty percent of the obtained method declare data is employed to teach the class model, and twenty percent is utilised for blind testing.

ORGANISATION OF THESIS

Chapter 1 **Introduction**

Bringing together computing and physical capacity, cyber physical systems (CPS) interact with humans in novel ways. It is not intended to function independently, but rather as a network of several variables with both physical input and output. Concepts like this have direct ties to computational intelligence-based sensor networks, which are increasingly used in fields like robotics.

Chapter 2 **Literature Survey**

For "the next model of approach which requires sparse integration of control technologies, communication, and computing to get equilibrium, robustness, reliability, performance, and then productivity inside battling genuine physical devices of numerous programme domains," CPS is the way to go. Because of their widespread application, CPSs have been the focus of

several committee meetings and reports aimed at identifying and addressing potential future challenges and opportunities.

Chapter 3 **Distributed processing in cps through novel shared computational model**

Combining computers, interaction, and equilibrium solutions, CPS is a networked real physical unit process. The task processing section of CPS makes use of transmitted technologies, and it places an emphasis on the interconnection between objects, machines, and people on the basis of environmentally friendly attention, which is secure, reliable, and cost-effective real-time detection or maybe command of an actual entity.

Chapter 4 **Anomaly detection in cps through effective parameter tuned dbn**

Sensors used in CPS for the purpose of facility monitoring and management are especially vulnerable to anomalies such as scalability failures, cyber-attacks, and other incursions. In order to detect anomalies and stop harmful actions, a powerful model called ADS has been used. False Positives (FP) also known as false alarms and False Negatives (FN) also known as missed forecasts are both experienced by ADS despite its great efficiency.

Chapter 5 **Dependability analysis on cps using machine learning techniques**

The resulting merger of physical information and processing techniques is a hybrid vehicle process that includes both physical and computer-defined (cd) elements. The systematic community has recently been interested in the research hubs of academics both domestic and foreign. In a nutshell, complex physical systems (CPS) are multi-dimensional methods that mix physical, communication, and computational environments. The system type programme is an elaborate distributed software application procedure that makes cross-device and cross-platform component references.

Chapter **6 Conclusion and Future Enhancement**

As a result of these efforts, we have developed a unique source characterisation framework and a method that facilitates the efficient distribution of application-specific tasks among CPS nodes. The dynamic availability and variety of computer components are hallmarks of such settings.

CONCLUSION AND FUTURE ENHANCEMENT

As a result of these efforts, we have developed a unique source characterisation framework and a method that facilitates the efficient distribution of application-specific tasks among CPS nodes. The dynamic availability and variety of computer components are hallmarks of such settings. The proposal takes into account areas such as setup preferences, flexible choice of computing materials inside CPS systems, private and corporate pcs, and additional capabilities arising from cloud technology to determine whether it is feasible and suitable. The framework also allows for therapies based on a wide variety of methodologies and technology, combining well-known, beneficial approaches with the most recent findings from research. The framework's provision for many instances of the different tasks required for the whole dispatched programme also has the effect of providing disappointment tolerance. This technique offers a flexible way of integrating computing resources and a range of organising options for allocating processing costs among CPS nodes, regardless of the underlying application: To lessen the cost of computing and to address security concerns, more and more organisations are turning to the cloud, but it's important to keep local resources safe for when they're needed most.

REFERENCES

[1] X.Dai, W.Chang, S.Zhao, & A.Burns. A dual-mode strategy for performance-maximisation and resource-efficient CPS design. ACM Transactions on Embedded Computing Systems (TECS), **18**(5s) (2019), page no 1-20.

[2] F.Qiao, J.Liu , & Y.Ma. Industrial big-data-driven and CPS-based adaptive production scheduling for smart manufacturing. International Journal of Production Research, **59**(23) (2021), page no 7139-7159.

[3] T.Yang, Z. Huang, H.Pen, &Y. Zhang. Optimal planning of communication system of CPS for distribution network. Journal of Sensors, 2017,page no 1-10

[4] X.Fei, N.Shah, N. Verba, KM Chao, V.Sanchez-Anguix , J.Lewandowski, & Z. Usman. CPS data streams analytics based on machine learning for Cloud and Fog Computing: A survey. Future Generation Computer Systems, **90** (2019),page no 435-450.

[5] L.Qi, Y. Chen, Y. Yuan, S.Fu, X. Zhang & X.Xu, A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web, **23**(2**) (**2020**)**, page no 1275-1297.

[6] M.R.Khosravi & V.G.Menon. Intelligent and pervasive computing for cyber-physical systems. The Journal of Supercomputing, (2020) page no 1-2.

[7] J.Goh, S.Adepu, M.Tan, Z.S Lee. Anomaly detection in cyber physical systems using recurrent neural networks. In Proceedings of the IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January (2017), page no. 140–145.

[8] A.M Kosek.Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model. In Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, 12 April (2016),page no 1–6.

[9] S.Krishnamurthy, S.Sarkar, A.Tewari. Scalable anomaly detection and isolation in cyber-physical systems using bayesian networks. In Proceedings of the ASME 2014 Dynamic Systems and Control Conference, American Society of Mechanical Engineers, New York, NY, USA, 30 October (2014), page no. V002T26A006–V002T26A006**.**

[10] C.Zhou, H.Luo, W.Fang, R.Wei, & L.Ding.Cyber-physical-system-based safety monitoring for blind hoisting with the internet of things: A case study. Automation in construction, **97**(2019),page no 138-150.

LIST OF PUBLICATIONS

1.S.Krishna Narayanan, S.Dhanasekaran & V.Vasudevan. An effective parameter tuned deep belief network for detecting anomalous behavior in sensor-based cyber-physical systems.S(2022) (Elsevier Publisher)

2.S. Krishna Narayanan, S.Dhanasekaran,. & V.Vasudevan. Depend Ability Analysis on CPS Using Machine Learning Techniques. Journal of Applied Engineering and Technological Science (JAETS), **5**(1) (2023), page no 339-348.

3.S.Krishnanarayanan, S. Dhanasekaran, &V.Vasudevan. A shared computational model using distributed processing in a CPS enabled environment. In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA) (2021) page no 841-846. IEEE.